Developing a Testing Framework for Internet of Things Devices

An Honors Thesis (HONR 499)

By

Michael Mykyta

Becca Liwosz

Thesis Advisor

Dr. David Hua

Ball State University

Muncie, Indiana

April 2018

Expected Date of Graduation

May 2018

Abstract

Security in the Internet of Things (IoT) devices is a large area of research in the technology field. The current default security on IoT devices is almost nothing. The research presented in this thesis is a baseline for finding the vulnerabilities in IoT devices. Once these vulnerabilities are found it is just a matter of getting the manufacturer of these devices to secure them during production. Most of these devices have very similar vulnerabilities to one another, but the method of fixing these issues can vary from device to device. The processes that were created during this research will hopefully be used to help with security for the everyday user.

Acknowledgments

I first want to thank my thesis partner Becca Liwosz for all the work she did to prepare and complete this thesis. This thesis could not have been completed without all the work that she put in to both create this document and keep me on track to finish this on time. I next want to thank our thesis advisor Dr. David Hua for introducing this thesis topic to us and providing assistance throughout the duration of this thesis. I also want to thank Dr. Hua and the other professors in the Computer Technology department for everything they have taught and assisted me throughout my time here at Ball State, those professors being Mr. Rob Turner, Ms. Patricia Lucas, Dr. Biju Bajracharya, and Dr. Christopher Davison.

Table of Contents

Process Analysis Statement

Security is something that has always been important to me in many facets of my life, whether it be a career, where I live, or the technology I own. My need for security is especially apparent when I make decisions regarding any technological purchases. The recent number of news stories regarding technological security breaches has only amplified my need for security, especially since it was big companies that were reporting that personal information was stolen. That is why this thesis is so important to me, because I wanted to have a chance to help improve the future of the security landscape. This thesis was my chance to not only leave an impact on an industry that I wanted to be a part of, but also to begin research that will hopefully be continued by future students.

When the idea for this thesis was first presented to me, I started to wonder how far this research could go. I wondered if we would have the chance to work with manufacturers to test new devices that had not hit the market yet or if we would have the opportunity to make our testing framework a new standard for security testers. It was and is still is too early to answer these questions, but the possibility that we could make a substantial impact on security testing allowed me to approach this thesis with more excitement than I would a typical school assignment. It became real when I realized that this could be more than a grade if our testing framework was ever adopted. This realization encouraged me to give this thesis my complete effort and make sure it was some of the best work that I had done while at Ball State.

The idea of leaving a legacy after I graduate was never a big concern for me, because my main worry was to make sure that I received a diploma after four years of school. This thesis made me question what my undergraduate legacy would be if I had not participated in creating an honors thesis. I assumed that my legacy would be as a statistic, adding to Ball State's

graduation rate or adding to the number of graduated honors students, but not for much else. This thesis would allow me to create a legacy for myself and potentially inspire future students to continue building on the framework that this thesis provides. I could start an effort that could potentially add to the technological education landscape and to the security testing landscape, something that I could not pass up. I may never know the result of the research that we started, but the idea that this thesis could lay the ground work for bigger things encouraged me to approach this thesis like it was one of the most important things I had ever done.

Before work could begin on our testing framework, first we had to do background research. This research involved assessing security measures that are currently being applied to Internet of Things devices as well as researching any possible frameworks that may have already been in place. Throughout my time doing this research, I was surprised at the lack of security that these devices were receiving. The Internet of Things is becoming very popular, especially since most people are using several devices that connect to the Internet. My research showed me that security was not always a priority for the companies that manufacture these devices, which drove myself to reconsider if I would purchase these devices in the future. If a company was not going to place a priority on my personal information, how could I purchase a device that was going to not only store my personal information but also use that information to adapt itself to my interests? I had previously been of the mindset that I have nothing to hide on the Internet, especially because I do not share that much on the Internet. My research forced me to challenge that mindset and become warier of the security of the devices that I use.

The research that I did allowed me to embrace my paranoid side, because I was never worried about what personal information I shared with my devices. I assumed that my information would be safe because companies made sure that my information would be secure. I

never worried if my device was using my information without my consent or if my device gathered more data about me than I had allowed it to. My research showed me that I had to worry about the information I chose to share with my devices, because the company that manufactured the device was not going to worry about it for me. My research made me reevaluate how I use my cell phone and what information I chose to share with the various applications that I have installed on my phone. I encouraged my paranoia, because I would be safer in the long run should one of my devices or a company that manufactured one of my devices be hacked. I carried this newfound paranoia into creating a framework and device testing so that I could make a comprehensive framework that would address every security concern within my assigned category.

After research was completed, we had to learn about the testing methods that could be used to assess the security of Internet of Things devices. This involved working with the operating system Kali Linux, a variation of Linux that was used primarily for security education and testing. I had previously worked with this operating system before in one of my classes, so I was able to carry over much of the information that I had learned in that class to this thesis. This information would need to be reinforced through several training sessions at the beginning of this thesis so that I would be fully prepared when we began testing our framework on the Internet of Things devices. The training proved to be valuable as I had forgotten some of the information that I had learned in previous classes, and after this training was completed our testing framework could then be created.

When we started to build our testing framework, we first broke down the different vulnerabilities or privacy concerns that we would be testing for. We asked ourselves questions that our framework would need to answer. For example, if we were assessing a password

complexity requirement for a certain device, we had to first ask ourselves what ideal password complexity requirements would be so that we make sure our framework would address that which we thought was important. This same method would be used for each concern until we had developed the basis that our framework would be built on. The framework that we then built sought to answer each of the questions we had asked without leaving any gaps. We made sure that each step we included would serve a purpose in answering a question, and that were no steps that seemed unnecessary. We also had to make sure that we included enough steps so that anyone could adequately follow our framework. One common problem that can be found in technical documentation is a lack of complete comprehension, meaning that there may be steps missing in the document because a manufacturer assumes that the user has knowledge that they do not have. This is a problem that we wanted to avoid, so we made sure that each portion of our framework would be tested before we considered it complete.

The testing portion of this thesis proved to be straightforward once our framework was complete. The devices that we chose to test with were able to be tested with the framework we had built, and our framework proved to be comprehensive and adaptable enough to work with several devices regardless of manufacturer. Since many devices use mobile applications as their platform for user configuration, the framework we built can be applied to a wide variety of Internet of Things devices. The adaptability of the framework also allows for expandability as well, since testing can be done almost anywhere if it can be done primarily with a smart phone and an Internet of Things device. This increases the impact of our framework as well because of the large popularity of smart phones. Many people own smart phones, and because Internet of Things devices rely on smart phones for configuration, this framework will be important in making sure consumers feel that the devices they purchase are safe.

The framework that I have helped build will hopefully not only have an impact on security testing in the future, but also has allowed me to examine myself both as a technological consumer and as a researcher. Functionality and features typically takes a lead role in determining what pieces of technology are worth purchasing, while security is usually an afterthought. This has been my mindset in the past when I have made some technological purchases. I embraced this mindset because I wanted to experience a piece of technology that I had not experienced before, more concerned with what the technology could do than if my information would be safe while I used the device. While the new technology may seem enticing because not many people have it, the security concerns regarding a new device need to be addressed before a purchase is made. This is the mindset that I want to strive to have when I look to make future purchases, so that I can make sure that my information will be safe with the device that I choose to purchase.

While this thesis taught me to embrace a more cautious mindset when making purchases, I also learned to embrace a more complete approach when doing research. In the past, I relied heavily on the database Academic Search Premier because it was what Ball State had introduced me to when I first started my undergraduate career. I had always used Academic Search Premier for research that was required of me prior to this thesis, because I was able to find everything I needed on that database. This thesis forced me to look elsewhere for my research, primarily because the Internet of Things is not a widely researched topic. I had been wary to use Google for research because I wanted to make sure all my sources would be academic sources, but due to the nature of my research I needed to use Google and Google Scholar to find all the sources I would need. This thesis taught me to not only take a more cautious approach when it comes to security, but also use all my resources when completing my research. These lessons and the

experience I have gained working on this thesis will be carried with me after I have graduated from Ball State, along with the feeling that the work I have been a part of will leave an impact both on Ball State and on the future of the security industry.

Introduction

When it comes to technology in today's world, it is a necessity for convenience and efficiency in everyday life. Almost everything is dependent on technology and going without it makes life much more of a hassle. Because of this, the users of technology just use it without actual knowledge of what kind of information the technology has. This is a huge issue in the realm of the Internet of Things (IoT). Because these devices are mainly household items that are easy to forget about, users do not usually think to check the security on these devices.

As far as the manufacturing of these devices goes, there is very little security built into the devices. This is a problem that needs to be solved because most users do not have the knowledge or ability to secure their own devices, which most likely leaves their personal information available for malicious users to find. Having better security as a default on these devices is a step towards helping protect user's personal information that might be stored on their IoT devices that they use every day.

Part of the process in this research was looking for vulnerabilities in these devices and finding ways the manufacturer could fix these vulnerabilities during production. This information could help streamline the process of securing future IoT devices and helping keep user's information private. One of the challenges of this process is that every device is different but most have very similar security issues. So finding those vulnerabilities is not difficult, but fixing them is a different process on every device.

There has been other research into the topic of IoT security. A big player in this research is the Open Web Application Security Project (OWASP) which has a more in depth list of categories that are being researched for all devices, not just IoT.

In this research there are two categories that are focused on from OWASP. Those are the two that were tested and researched during this thesis.

Literature Review

One of the biggest questions from people looking at this area of technology is, what is IoT? IoT stands for the Internet of Things and it encompasses everything that is considered a "smart" device. More and more, things are being connected to the Internet to bring some type of functionality to the user. One article describes the Internet of Things as a source of "unprecedented opportunities to penetrate technology and automation into everything we do, and at the same time, provide a huge playing field for businesses to develop newer business models to capture market share" (Kumar, Murthy, 2015)

It appears more and more everyday objects have Internet access, from your phone to your refrigerator and even your doorbell. This can be a great benefit to consumers, because it can make their lives much more convenient and easy to manage. There is a downside, of course. The downside is that with all these devices that have access to the Internet, there are many ways that a person with malicious intent can access a user's personal information. Most of the average users of these various technologies are not informed enough to even know that they need to protect themselves from this type of threat. This makes what was originally a large threat, exponentially larger. That is where education of users becomes extremely important.

Education of users is an interesting subject. Because it is so important for users to know how to protect themselves. The company's manufacturing these devices should have built in security measures that protect users even if they are not aware of the risks involved. Many IoT devices that are sold to customers every day have very large security risks built into them that could be easily closed during the manufacturing process. Many devices that have been looked at in this survey have had direct Telnet access on them. This means that a user with malicious intent could access the device and find the credentials of the user and other information that are stored on the device. This is a very simple thing to close during the manufacturing process. This alone would help protect many users from malicious hackers. There are other things that can be done on the manufacturer's side to protect users that simply are being ignored. This is an issue that will become more and more prevalent as IoT devices increase in popularity as the years go on.

"The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally." (Chapin, Eldridge, Rose, 2015)

The scope of IoT is enormous. When the average user thinks of the Internet of Things they think of the household items that are on the market, which is a huge area of IoT, but it is not the largest. There are even more opportunities for growth in the business and development side of this field. "From the point of view of a private user, the most obvious effects of the IoT will be visible in both working and domestic fields. In this context, assisted living, smart homes and offices, e-health, enhanced learning are only a few examples of possible application scenarios" (Bandyopadhyay, Sen, 2011) This is a good summary of what IoT can accomplish, and there is even more that can be accomplished and will most likely become more popular in the future. The fact that IoT has such a huge scope makes it even more important to educate users on the security

risks that come with use IoT devices on a regular basis. Especially when they are being used more and more in the medical fields. This scope is growing exponentially as time goes on. In 2015 there were an estimated 15.4 billion devices is use and it is predicted that this number will grow to over 75 billion by the year 2025. (Statista, 2018)

There are even bigger aspirations when it comes to the scope of the Internet of Things. Cloud computing brings in even more layers of complexity to these devices, but it also allows users to do even more with these devices. "Cloud computing offers a new management mechanism for big data that enables the processing of data and the extraction of valuable knowledge from it." (Al-Fuqaha, Ayyash, Aledhari, Guizani, Mohammadi, 2015) This source goes on to talk about how adding the cloud into the IoT equation allows big data to be used. Big data is another concept that I will not go into in depth at this moment. But basically, it is taking huge amounts of data that are available on the internet and using that as a tool to solve problems. This concept of big data is enhanced greatly by the concept of IoT. This is because with IoT there is a huge amount of data available that was not available before. This adds to the security issue that was discussed before, which is that there is so much personal data from user's devices that can be used against them by a malicious user. Just another reason to educate users on what kind of information is accessible from the devices that they use every day.

The scope of the Internet of Things is ever expanding, and this also reflects the growth that IoT is undergoing. The Internet of Things was first popularized with the rise of smartphones, as cell phones were now able to connect to the Internet and act as a computer. This set the stage for companies to incorporate this new technology into already existing technologies as well as create new devices that can communicate over the Internet. In an interview with the New York Times, Tim O'Reilly lists Uber as an early adopter of the Internet of Things, since they are "a

company built around location awareness" using the cell phone of both the passenger and the driver (O'Reilly, 2015). The two cell phones communicate with each other, letting the driver know where the passenger is and the passenger when the driver will arrive (O'Reilly, 2015). Uber's early adoption of IoT has since been expanded by other companies to further learn more about their customers.

This expansion can be shown through Google Now, which was created by Google as a personal assistant. While speaking about Google Now, O'Reilly says that "it has context awareness, alerts and knowledge of my preferences" (O'Reilly, 2015). This expands beyond the idea of location awareness, as now Google can use the information on a smartphone to give recommendations to customers based on past Google searches, their mobile applications, and location among other things. This expansion of IoT can only be expected to grow as more devices become smart and connected to the Internet, such as household appliances as mentioned earlier. Devices will continue to become smart, and as a result the Internet of Things will continue to grow and learn more about the average consumer.

As the Internet of Things grows, so too does the need for security. The Internet of Things, upon its inception, was not widely adopted and as a result security was not seen as a priority to the companies making the devices. This is mainly because security added an extra cost to the manufacturers producing the devices, who viewed security "as a loss leader" because of low consumer demand for security (Wright, 2017). Now that the Internet of Things is growing, security is becoming more of a concern especially for companies trying to market their product to consumers. In the article "Mapping the Internet of Things", Alex Wright mentions that "wherever the Internet goes, security risks seem to follow. As the Internet of Things (IoT) continues to expand, those risks are taking on new dimensions well beyond the familiar threats of

stolen passwords and credit cards" (Wright, 2017). These new risks can be shown through Shodan, a search engine that is designed to monitor the security of "nearly four billion devices over the IPv4 network" (Wright, 2017). Shodan collects data on Internet of Things devices by monitoring several "TCP/IP-connected ports including FTP, SSH, SNMP, SIP and RTSP ports" (Wright, 2017). This data is then used to find vulnerabilities that may affect the scanned devices.

The data Shodan has found has uncovered vulnerabilities in "more than 100,000 IoT devices in 2011", opening these devices "to attack by 'malicious actors'" (Wright, 2017). One attack that hackers have been able to employ with Internet of Things devices is a Distributed Denial of Service attack, or DDoS for short. In a DDoS attack, hackers use infected devices as bots to overload an online service, causing it to crash. This attack can halt business operations, leading to lost revenue and a potential loss of customers. The Internet of Things reduces the difficulty of executing DDoS attacks because of the large number of potential bots, reducing the need for one device to create a large amount of traffic. This makes it so "amplification is not necessary" since many devices in several different locations can create an overflow of traffic instead of "a single packet producing a much more massive reply" (Lemos, 2016). These DDoS attacks are also "difficult to stop because they are coming from so many corners of the Internet and not from known bad Internet addresses" (Lemos, 2016). The insecurity of Internet of Things devices will only allow these attacks to become more prevalent "and future attacks will likely be much worse" because "manufacturers have not stepped up to secure their devices" (Lemos, 2016). The lack of security as well as the dispersion of Internet of Things devices will only cause hackers to continue to find new vulnerabilities for these devices, leading to a need to more heavily secure the devices before they are released to the public.

The need for security in the Internet of Things can also be shown through the potential outcomes that could arise should these devices remain vulnerable. The Belkin WeMo, a smart power outlet, was found with three flaws by "researchers from security research group Invincea Labs" (Lemos, 2016). One of these flaws would allow "attackers to remotely install code on the devices," which could in turn give an attacker "a higher level of access than you can have as a valid user" (Lemos, 2016). This attack can be hard to defend against because the user does not have high level administrative access to the device, making it "almost impossible for the user to remediate this type of attack" (Lemos, 2016). This attack could lead to a home being broken into remotely and a loss of customers for Belkin. The ability of attackers being able to access home devices could extend into more devices in the future, with attackers potentially able to steal personal information found on the Internet through IoT devices. Attackers already can bring down parts of the Internet, and in the future attackers may be able to steal personal information over the Internet using IoT devices as well. The outcomes of low security can be severe, and as a result security needs to become a higher priority for manufacturers.

The low security of Internet of Things devices is not a new topic of concern, as there have been several cases where these devices have been known to have vulnerabilities. A cardiac device from St. Jude Medical was found to "have vulnerabilities that could allow a hacker to access a device" (Larson, 2017). The effect of this could be life-threatening, since the attackers "could deplete the battery or administer packing or shocks" (Larson, 2017). This vulnerability was eventually fixed by St. Jude, but it took over a year and several legal battles before St. Jude would admit the security flaw and fix it (Larson, 2017). Security needs to become a priority for companies as IoT continues to grow, especially if these companies want to maintain their customer base.

There are steps currently being taken to secure IoT devices. The issue that is very common in IoT devices is that they have the protocols that they need to be secure, those protocols are just often not in use by default. Users might or might not have the ability and access to change these protocols on their devices. Also, most users are not knowledgeable enough to know how to access these protocols and enable or disable them appropriately. So manufacturers are able to easily increase the security on devices, it just does not happen often.

The manufacturer of these devices most likely leave these protocols open to make creating the devices easier to configure when they are being made. The access that they have is extremely wide. "As these devices are connected to the Internet, they can be reached, and managed at any time and at any place" (Keoh, Kumar, Tschofenig 2014). Because these devices have so much access to everything it makes security difficult. But this is a problem that can be stopped at the beginning of the entire process.

The topic of security when it comes to building it into IoT devices is also interesting when it comes to independent verification. Independent verification can be things like Wi-Fi. These independent entities are what devices go through to get approved for public use. With Wi-Fi as an example, devices that manufacturers want to have Wi-Fi enabled on them need to get looked at and approved by the Wi-Fi Alliance. Many different companies and industries work with the Wi-Fi Alliance to bring people the Internet that they depend on every day. This process can be long but it is worth it to bring Wi-Fi to those who desire it. Devices are checked to make sure that they have everything that they need to have Wi-Fi and run it correctly and once they have the Wi-Fi Alliance stamp of approval they are moved into production and onto the consumer. There are independent verification entities for security as well, such as ISO. These can be used in the IoT world to improve security before the device even gets to the user.

Manufacturers could make independent verification part of the manufacturing process to help the users.

One of the main security players in the software field is the Open Web Application Security Project (OWASP). This is a project that has a goal to improve the security of all software and can be used to help secure the software of IoT devices. OWASP can be a large resource for IoT security as a whole. The reason for this is because they have guidelines already in place for security and penetration testing that can be used to help IoT devices in that area. OWASP can be used as a resource to bring the devices up to standard when it comes to their security vulnerabilities.

Currently there is not a standard for security when it comes to IoT devices. This is mostly likely because they are newer devices and the technology world has not taken the time to standardize them as of yet. This can be and needs to be changed because the lack of security on IoT devices is becoming harmful to users.

Research Question

OWASP lists several Internet of Things vulnerability categories on their website that manufacturers should look for when producing new devices. The categories that will be covered in this thesis include Privacy Concerns and Insecure Web Interface Protocol. OWASP provides a general outline for testing their listed vulnerabilities, but the testing procedure is largely left up to the manufacturer. As a result, the procedures are not standardized for all devices and can leave some gaps in testing. The purpose of this thesis is to develop a set of procedures to assess the security of IoT devices for the OWASP IoT vulnerability categories listed above.

Methodology

Privacy concerns is a category of OWASP that is a large part of the security issues with IoT. This category of OWASP deals mainly with the personal information of the user of the devices. When it comes to IoT, there is a lot of personal information that is collected by these devices. If a device were to be compromised there would be a lot of personal information that could be gathered about a user. This is also true when it comes to the manufacturer itself being compromised. The manufacturer might have all of its user's information that a malicious user could possibly gain access to. This type of information is the thing that should be secured at all levels. Things like encryption and security policies are needed to protect user's information. These are discussed in the next steps.

- The first topic that should be explored when it comes to privacy concerns is ensuring that only the minimal amount of person information is collected from consumers. Below are steps to see how this could be impacting an IoT device.
    - How much information is being asked for upon account creation?
        - Things like home address or credit card information or birthday.
        - Any information that is not critical to the device operation should not be provided.
    - Can someone who does not own the device see the users information?
        - Can you reset someone's password without their permission?
        - Can you call the company and get information about another user?
    - Can someone see the users information from their own device?

        - Attempt to SSH or Telnet into another device and see the user's information.
        - Attempt to "pair" with another device and gain information through the manufacturer's app on the device.
        - If there is a USB port, attempt to directly connect to the device and get the user's information off of it.

- Another topic that should be looked at is ensuring that end-users are given a choice for data that is collected beyond what is needed for proper operation of the device. Below are steps to check this topic.
    - Attempt to turn off the location service on the device if it is not needed.
    - Is there a way to manually turn off all of the services that are not needed on the device?
        - Attempt to shut off services like the camera, contact sharing, photos, microphone, and the calendar
    - Can the manufacturer be contacted about this issue?
        - Call or email the manufacturer if you cannot turn off these services and ask if they can turn them off for you.

- No matter what IoT devices need to have some personal information about the user. The steps below tell how to ensure all collected personal data is properly protected using encryption at rest and in transit.
    - Man-In-The-Middle Attack.

        - See if the data collected in the Man-In-The-Middle is in clear text or not
    - Test if Telnet is enabled.
        - This is not an encrypted protocol.
    - Try and change the password of an account that belongs to another user and see if it is listed in clear text anywhere.
    - Check if SSH is enabled on the device.
        - Any unfamiliar device should not be able to SSH into the IoT device.

- Another method of keeping personal information safe is to ensure that only authorized individuals have access to collected personal information. This can be tested by performing the following actions.
    - Are accounts password protected?
        - Was the user forced to make a password upon account creation?
        - Are there minimum requirements for the password such as number of characters or special character requirements?
    - How easy is it to gain access to an account?
        - Can I reset another account's password easily?
    - Is personal information tied to a public profile?
        - Attempt to find other profiles from that specific manufacturer.
        - Is there user information available on the manufacturer's website?
    - Can a user see other people's information from their own account?
        - From your own account, attempt to connect with other users' profiles.
    - Can a user control how much information is shown as public in their profile?

        - Attempt to alter the privacy settings on your account.
    - Do a Man-In-The-Middle attack and see if other users credentials are available
    - Try to establish a Telnet or SSH connection to the device and find the users information

- If a manufacturer is using user's personal data for studies or any other reason the data should be de-identified or anonymized. This means that all of the personally identifiable information is taken out of the data that is used.
    - Call the manufacturers and ask what their policies are on anonymizing data
    - Explore the survey sites that are being used by the manufacturer and see if the data being used has any personally identifiable information in it.

- One question that should be asked of the manufacturer is if a data retention policy is in place. If data is kept too long that can be a security risk. The tasks below tell how to check if a policy like this is in place.
    - Call the manufacturers and ask what their policy is
        - Are they keeping users data?
        - How long are they keeping users data for?
        - Where are they keeping the user's data and is it encrypted?
- Web interface vulnerabilities can be more difficult to test for because there are so many different types. Below are a few of the more common ones.

- XSS. This is Cross Site Scripting, which occurs when a malicious user tricks another user into running a script on their device. Below are some steps to test for XSS vulnerabilities. (Weber, 2005)
  - Map out the site and how it works.
  - Find all of the points of user supplied input.
  - Test tools like Paros proxy and Fiddler on these points.
- SQLi. This is a vulnerability that involves bad SQL code that manipulates the SQL database in a device and shows information that was not meant to be displayed. Below are steps provided to test this issue. (Incapsula, 2008)
  - Manipulate a standard SQL query to exploit existing variables.
  - See how the system responds.
- CSRF. This stands for Cross Site Request Forgery attack. This is a method that tricks a web browser into running an unwanted script or action. Below are some steps to test for this vulnerability. (Incapsula, 2008)
  - Study the application to make the request as legitimate looking as possible.
  - Send a CSRF to the device.
  - See if the device accepts the request or if it warns the user that it might be a bad link.

The insecure web interface protocol is a category of IoT Security Guidance for OWASP, or the Open Web Application Security Project. This protocol discusses the web interface that one would use to interact with an IoT device. This could be a mobile application or a webpage within a browser. The guidelines that OWASP provides regarding this protocol help manufacturers,

consumers, and developers know what they should be looking for in the devices they are either buying or producing. The inability to follow the guidelines may result in a device itself or user accounts being compromised, which could result in many users losing their personal information or control over the device that they own. The follow is a list of the guidelines that OWASP provides as well as ways to test whether the guidelines are being followed.

- The first guideline is assess any web interface to determine if weak passwords are allowed. This guideline focuses on the password complexity requirements that a web interface implements, if complexity requirements are even implemented. The following are steps that assess whether a web interface has properly implemented password complexity requirements:
    - Try using "password" as the password.
    - 1. Download the application that corresponds with the device being used.
    - 2. The application will prompt for a sign-in upon first entry. Select the option that allows for account creation.
    - 3. Follow the initial steps for account creation, such as entering an email and username.
    - 4. After the initial steps are completed, the user will be prompted to create the password for their account.
    - 5. Attempt to enter several weak passwords, such as "password," "abcd," or "123456." If the account creation allows for these passwords to be created, then weak passwords are acceptable.

- 6. If the application does not accept these passwords, there is a password complexity policy in place such as a minimum length requirement or a requirement for special characters.
- 7. Document whether the application allows for weak passwords. If the application does not allow for weak passwords, document the password complexity requirements that are in place.

- The second guideline is assess the account lockout mechanism. This guideline focuses on a web interface's attempt to lock a user out if incorrect account credentials are entered a given number of times, if the interface attempts a lockout at all. The following steps will help assess whether a web interface does lock a user out after several failed login attempts:
  - Attempt to log into the device with a legitimate username and an invalid password 3 times in rapid succession. Then try to log in with the correct username and password.
    - If it does not allow login, then an account lockout mechanism is in place.
    - If it does allow login, repeat invalid login with an increasing number of login attempts up to a maximum of 10.
    - If able to login after 10 success attempts, the assumption is that there are no account lockout mechanisms.
  - 1. Download the application that corresponds with the device being used.
  - 2. The application will prompt for a sign-in upon first entry. Select the option that allows for account creation.

- 3. Follow the steps for account creation.
- 4. Once the account has been created, log out of the application.
- 5. Attempt to log back into the application with the correct username and an incorrect password.
- 6. Repeat these login attempts until 10 attempts have been reached. If the account has not been locked out after 10 attempts, then an account lockout mechanism is not in place.
- 7. If the account did lock after several incorrect login attempts, document the number of attempts that were allowed before the account locked. If the account did not lock, document that an account lockout mechanism is not in place.

- The third guideline is assess the use of HTTPS to protect transmitted information. This guideline focuses on whether the web interface is secure through the use of HTTPS. The following steps assess whether the web interface uses HTTPS through the use of web certificates:
  - 1. Open the web interface for the device being tested.
  - 2. If the web interface is within a browser, look in the address bar for a lock. If there is a lock then HTTPS is being used. Document whether the interface is using HTTPS.
  - 3. Many browsers will also show the status of certificates being used on the web interface. If the browser allows, click on the lock and select the option that corresponds with the web certificate.

- 4. View the status of the web certificate. If given, document when the web certificate will expire.
- 5. If information on the web certificate or it is not apparent that HTTPS is being used, contact the manufacturer to ask if they secure their web interface.

- The fourth guideline is assess the ability to change the username and password. This guideline focuses on the ability of a user to change the username and password that belongs to that account, especially assessing the ease at which this can be done. The following steps are a guide to changing the username and password of a created user account for a given IoT device:
  - 1. Download the application that corresponds with the device being used.
  - 2. The application will prompt for a sign-in upon first entry. Select the option that allows for account creation.
  - 3. Follow the steps for account creation.
  - 4. Once the account has been created, log out of the application.
  - 5. On the application login screen, select the option that asks if a password has been forgotten.
  - 6. The application may take one of several approaches to changing account information, including changing the password within the application or via email. Follow the steps given by the application. Document the method that the application used to reset the password.
  - 7. Login with the new password created.

- 8. After a successful login, navigate to Account Settings within the application if it exists.
- 9. Once on the Account Settings screen, select the option to change username or password if the option exists. Follow the steps necessary to change the username or password.
- 10. Document the method the application used within Account Settings to change either the username or password.

- The last guideline is determine if web application firewalls are used to protect web interfaces. This guideline focuses on how accessible web interfaces are to potential hackers. The following steps assess the ease of access that a web interface allows through the use of a port scan:
  - 1. Open a command prompt or terminal window, depending on the operating system that is being used.
  - 2. Run an nslookup to get the IP address of the web interface.
  - 3. Once the IP address has been found, run a port scan on the IP address using nmap. The results of this scan will show what ports are open and closed.
  - 4. If there are closed ports, then the web application is using a firewall to protect the web interface. If there are no closed ports, then there is not a firewall in place.
  - 5. Document the results of the port scan, making sure to note which ports are open on the device.

Conclusions

As stated in the research question, the purpose of this thesis was to provide a security testing framework for Internet of Things devices for the OWASP Privacy Concerns and Insecure Web Interface Protocol vulnerability categories. OWASP provided testing suggestions on their website, but a comprehensive testing guide was needed to ensure that all Internet of Things devices receive the same level of security testing. The security testing framework that this thesis provides gives manufacturers and security testers a comprehensive step-by-step guide for use when testing existing and future Internet of Things devices. Consumers can also gain some peace of mind in knowing that there are now existing testing frameworks for the devices that they may purchase in the future.

The testing framework that this thesis provides adequately addresses two OWASP Internet of Things vulnerability categories, but there are still categories that will need to be addressed in future frameworks. There are ten categories in all, and these will need to have testing frameworks established in the future to ensure that future Internet of Things devices will be secure. Future students can use the existing frameworks to create new frameworks for the remaining OWASP vulnerability categories. When all frameworks have been created, a comprehensive testing guide can be created which will contain every testing framework for every OWASP vulnerability category. Once a comprehensive framework has been created, then manufacturers and security testers will be worked with to start to establish the testing guide as a new standard. This new standard will allow all future manufacturers and security testers to fully test any new and existing devices. This thesis is an important first step to more comprehensive security testing, but there is still more work that needs to be done if manufacturers want to produce fully secure devices and ensure their consumers that the devices they purchase are safe.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347-2376.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *Computers and Communication (ISCC), 2015 IEEE Symposium on* (pp. 180-187). IEEE.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, *58*(1), 49-69.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, *61*(3), 527-542.

Incapsula, (2008). Cross Site Request Forgery (CSRF) Attack. Retrieved April 20, 2018 from https://www.incapsula.com/web-application-security/csrf-cross-site-request-forgery.html

Incapsula, (2008). SQL (Structured Query Language) Injection. Retrieved April 20, 2018 from https://www.incapsula.com/web-application-security/sql-injection.html

Jain, P. (2012). Security Issues and their solution in cloud computing. *International Journal of Computing & Business Research*, 2229-6166.

Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal*, *1*(3), 265-275.

Larson, S. (2017, January 9). FDA confirms that St. Jude's cardiac devices can be hacked. Retrieved April 4, 2018, from http://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/index.html

Lemos, R. (2016). IoT Devices Evolving Rapidly as Favorite DDoS Attack Tool, Experts Say. *EWeek*, 1–1.

Murthy, D. N., & Kumar, B. V. (2015). Internet of Things (IoT): Is IoT a Disruptive Technology or a Disruptive Business Model?. *Indian Journal of Marketing*, *45*(8), 18-27.

O'Reilly, Tim. (2015, February 4). Explaining the Internet of Things - Science in Context [New York Times]. Retrieved from https://goo.gl/q8cWCK

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC)*, 1-50.

Statista (2018). *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).* Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Tsipenyuk, K., Chess, B., & McGraw, G. (2005). Seven pernicious kingdoms: A taxonomy of software security errors. *IEEE Security & Privacy*, *3*(6), 81-84.

Ukil, A., Sen, J., & Koilakonda, S. (2011, March). Embedded security for Internet of Things. In *Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on* (pp. 1-6). IEEE.

Weber, C. (2005, May 6). Testing Your Web Applications for Cross-Site Scripting Vulnerabilities. Retrieved April 20, 2018 from https://technet.microsoft.com/en-us/library/cc512662.aspx

Wright, A. (2017). Mapping the Internet of Things. *Communications of the ACM*, *60*(1), 16–18. https://doi.org/10.1145/3014392